Security Channels

Published by the
Air Force Special Programs Security Education Council

3rd Quarter 2001

Personnel Security
- Your Responsibility to Protect Classified Information -

Lets take the opportunity to review one of the most important documents each of you signed when you initially came on board -- your Briefing Acknowledgment Form. (BAF). Your BAF is your commitment, in writing, to assume the responsibility required to protect national security information in accordance with applicable Executive Orders and United States Codes (USC). Each person who programs signs one. This agreement takes effect the day you sign it, and continues even after you are debriefed. Take a moment to review the highlights of your BAF provided in the graphic below.

The Promise You Made
- To Live Up To Standards -

Another one of the promises we make when granted the clearance is to live a lifestyle consistent with the demands of trust. Before anyone is handed national defense information, they are evaluated against standards of personal behavior and conduct to ensure they have "what it takes" to protect our national security. An *adjudication process* carefully examines a sufficient period of each persons life to make an affirmative determination that the individual is an acceptable security risk. *The whole person* concept is used to weigh a number of variables that ensure the individual is trustworthy, reliable and loyal to the United States. All available, reliable information, past and present,

BRIEFING ACKNOWLEDGMENT FORM

1. *I am aware that the unauthorized disclosure of information could cause serious or grave damage to the National Security and that the unauthorized transmission or revelation of such information could subject me to prosecution under espionage laws and other federal criminal statues or applicable laws.*

2. *I do solemnly swear or affirm that I will never divulge, publish or reveal by word, conduct, or other means* such information or knowledge except when necessary to do so in the performance of my official duties in connection with the program/study and in accordance with the laws of the United States, unless specifically authorized in writing in each and every case by a duly authorized representative of the U.S. government.

3. *I understand that all conditions and obligations imposed upon me by this agreement apply during the time I am granted access and all times thereafter.* I have read the agreement carefully and my question, if any, have been answered to my satisfaction. **I acknowledge that the briefing officer made available to me Sections 641, 793, 794, 798, 952, and 1001**

Your Name Here

In this issue:

Highlight On
*** * Personnel Security * ***
AIS Security Education Corner
Editor's Corner
Policy Corner

continued from previous page

favorable and unfavorable, is considered when reaching the final determination. The evaluation involves considering all changes that life brings and ensuring those changes do not adversely impact the ability to safeguard national security information.

Again, ALL reliable information is used during the adjudication process. Adverse information concerning a single criterion may not be sufficient for an unfavorable determination. On the other hand, recent or recurring patterns of questionable judgement, irresponsibility, or emotionally unstable behavior are taken into consideration when evaluated against the guidelines.

The 13 Guidelines

The standards of personal behavior are identified in 13 separate guidelines. Each of the one has conditions that could raise a security concern and may be disqualifying, as well as conditions that could mitigate security concerns. Take a moment to review the 13 guidelines.

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Criminal Conduct
- Drug Involvement
- Emotional, Mental, and Personality Disorders
- Security Violations
- Outside Activities
- Misuse of Information Technology Systems (computers)

A Continuing Evaluation

It is important to remember that the evaluation process is not a one time deal. Throughout a career with classified information, each candidate must continue to prove that they are trustworthy, reliable and loyal. They must continually meet the spirit and intent of the 13 guidelines.

Accurate information is the key component for a successful continuing evaluation program. Changes to personal and pertinent work related information must be submitted to security on an ongoing basis. Most of the changes to personal information gets into your file because you put it there. Many of you have this memorized, but for those who do not, here's a reminder of what should be reported.

Reportable Personal Information

- change of name,
- change in marital status,
- termination of employment,
- change in citizenship,
- foreign travel (for personal or business reasons),
- foreign contacts (those that go beyond common courtesy or normal business

A Note from the Editor - Personal Responsibility -

If you think you aren't an important part of program protection, think again!

You're not only important, you're vital! And your responsibilities go far beyond locking a safe or logging off a computer.

As a hand-selected and adjudicated member of this team, you are charged with protecting vital national security information. You must be constantly in tune with your teammates and recognize changes in their personality or behavior that may possibly be an indicator of unauthorized activities, and in the most serious cases, espionage.

Your responsibilities also include taking responsibility for your own actions. Keep in mind that when you sign up to work on a program that involves protecting national secrets, you must personally do everything you can to minimize the threat to yourself. This doesn't mean you can't have friends, travel to distant lands or make a big item purchase. But we do want to caution and remind you, as we have throughout this newsletter and in our recent *Special Report* on Elicitation, that you must take seriously your responsibility to report information to the security office and take seriously the attempts made to gather information about you and your work.

No one in our community is exempt from these responsibilities. Initiating contact with foreign nationals or boasting about your "gee wiz" know-how to a neighbor could be viewed by some as a callous disregard for the sensitivity of these programs. From some perspectives, this might make you appear as more "approachable."

Take your [illegible] responsibilities seriously because the consequences of [illegible] could be very grave indeed.

Barry Hennessey
Security Director

Reporting Fraud, Waste

Everyone has a personal responsibility to report actual or perceived fraud, waste or abuse situations. No one is excused from the responsibility to report, but remember security when making the report. Due to the strict security rules in the community, we are required to make and handle these reports through protected channels.

Cases of fraud, waste and abuse should first be reported to supervisors. If appropriate action is not taken, or the situation is such that you do not feel confident discussing it with your supervisor, then you should call the community's fraud, waste and abuse hotline. It is the number is posted throughout your program area. If it is not, contact your security officer immediately!

The "800" number is answered by briefed individuals so it is possible to discuss classified information in a secure mode. All reports will be acted upon immediately. Confidentiality can be provided.

If you are aware of the fraud, waste a[illegible]orting [illegible]ct [illegible]ely.

AIS Security

Lets talk computer criminals. In 1993 the *Son of Slammer* study was initiated to study those individuals with a proclivity for computer crime. Why did the US government study computer criminals in such depth?

Not long before the *Son of Slammer* study, a young hacker broke into Air Force Pentagon computers. During sentencing negotiations between the hacker's attorney and the U.S. Attorney's office, the defense attorney advised the perpetrator not to plead guilty to a felony charge. He felt to do so might inhibit the young hackers change of getting a DoD clearance at a future date (he had actually considered working for the government!) and may possibly even hamper his chances of going to college to get a computer science degree. Law enforcement professionals in the area stepped in to state that, *"sending a computer criminal to college to get a computer science degree would be like sending a drug dealer to college to become a pharmacist."* They supported their comment by suggesting that, as with other crimes, breaking into computers or using computers to conduct criminal activity was "addictive behavior". When asked to validate the comment with supporting evidence -- there was none. Thus the *Son of Slammer* study was initiated. A behavioral psychologist was at the helm to conduct in-depth interviews with computer criminals in order to obtain a better understanding

continued

Son of Slammer is a dated study, but still contains valid conclusions. When the study results are married to our 21st century hi-tech working environment, we find that computer crime is not only present, but has been on the rise for quite some time.

The 13 guidelines that you reviewed previously in this newsletter even point to computer misuse as an indicator of inappropriate behavior. The opportunity has always presented itself for computer misuse and abuse, but crossing the line is unacceptable.

For those who do not cross that line, but who live in an environment where sloppy security practices such as password sharing and loose media control procedures are tolerated, you have created an open door for computer misuse, abuse and criminal acts to occur.

Poor AIS practices cannot and will not be tolerated within our work environment. Contact your ISSO if you have questions about security practices or what to report.

In the Next Issue:

* Highlight On Information Security *
Education Corner
Security Review Crosstalk
Editor's Corner
AIS Security
Policy Corner